



[CSRC Homepage](#)

[List of Acronyms](#)

## NIST Special Publications

Computer Security Resource Center - CSD

### 800 Series

#### Projects

- Cryptographic Standards & Applications
  - [Advanced Encryption Standard](#)
  - [Cryptographic Toolkit](#)
  - [Encryption Key Recovery Demo. Project](#)
  - [Public Key Infrastructure](#)
  - [Random Number Generator](#)

#### Security Testing

- [Automated System Security Evaluation Tool](#)
- [Cryptographic Module Validation Program](#)
- [IPSec](#)
- [NIAP](#)

#### Security Research & Emerging Technology

- [Authorization Management & Advanced Access Control Models](#)
- [Critical Infrastructure Protection Grants Program](#)
- [Common Criteria](#)
- [ICAT Vulnerability Database](#)
- [IPSec](#)
- [Mobile Ad Hoc Network Security](#)
- [Mobile Security](#)
- [Smart Card Security and Research](#)

#### Security Management & Guidance

- [Program Review for Information Security Management Assistance](#)
- [Policies - Federal, Directives](#)
- [Return on Investments](#)
- [Security Guidance](#)

#### Outreach, Awareness & Education

- [Awareness, Training & Education](#)
- [ISPAB](#)
- [Federal Agencies Security Practices](#)
- [Federal Computer Security Program Managers' Forum](#)
- [Small Business Computer Security Workshops](#)
- [FISSEA](#)
- [Archive of NISSC](#)

#### News & Events

- [Federal News](#)
- [Security Events](#)

#### Services For the:

- [Federal Community](#)
- [Vendor](#)
- [User](#)

#### Links & Organizations

- [Academic](#)
- [Government](#)
- [Professional](#)
- [Additional Links](#)

Draft SP  
800-72

*[Draft NIST Special Publication 800-72, Guidelines on PDA Forensics](#)*

Draft SP  
800-70

*[Draft NIST Special Publication 800-70, The NIST Security Configuration Checklists Program](#)*

Draft SP  
800-68

*[Draft NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist](#)*

SP 800-67

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher,  
May 2004

[Adobe .pdf](#) (960 KB)

Draft SP  
800-66

*[DRAFT Special Publication 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule](#) is still a DRAFT Publication - [click here to go directly to the DRAFTS page on CSRC.](#)*

Draft SP  
800-65

*[DRAFT Special Publication 800-65: Integrating Security into the Capital Planning and Investment Control Process](#) is still a DRAFT Publication - [click here to go directly to the DRAFTS page on CSRC.](#)*

SP 800-64

Security Considerations in the Information System Development Life Cycle,  
October 2003  
(revised file posted July 7, 2004)

[Adobe .pdf](#) (1,083 KB)  
[Zipped .pdf file](#) (669 KB)

SP  
800-63

Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology,  
June 2004

[Adobe .pdf](#) (217 KB)

**General Information**

- [Site Map](#)
- [Virus Information](#)

**Search CSRC** **Search Vulnerability  
Archive**

Enter vendor, software, or keyword

 

---

**SP 800-61** Computer Security Incident Handling Guide,  
**January 2004**

[Adobe .pdf](#) (2.71 MB)  
[Zipped .pdf file](#) (1.6 MB)

---

**SP 800-60** Guide for Mapping Types of Information and Information Systems to  
Security Categories,  
**June 2004**

[Volume I Adobe .pdf file](#) (444 KB)  
[Volume II: Appendixes Adobe .pdf](#) (2,003 KB)

---

**SP 800-59** Guideline for Identifying an Information System as a National Security  
System,  
**August 2003**

[Adobe .pdf](#) (95.5 KB)  
[Zipped .pdf file](#) (72.9 KB)

---

**Draft SP 800-58** *DRAFT Special Publication 800-58 : Security Considerations for Voice Over IP Systems is still a DRAFT Publication - [click here to go directly to the DRAFTS page on CSRC.](#)*

---

**Draft SP 800-57** *DRAFT Special Publication 800-57 Recommendation on Key Management is still a DRAFT Publication - [click here to go directly to the DRAFTS page on CSRC.](#)*

---

**Draft SP 800-56** *DRAFT Special Publication 800-56, Recommendation on Key Management is still a DRAFT Publication - [click here to go directly to the DRAFTS page on CSRC.](#)*

---

**SP 800-55** Security Metrics Guide for Information Technology Systems,  
**July 2003**

[Adobe .pdf](#) (569 KB)  
[Zipped .pdf file](#) (465 KB)

---

**Draft SP 800-53** *DRAFT NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems is still a DRAFT Publication - [click here to go directly to the DRAFTS page on CSRC.](#)*

---

**SP 800-51** Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability  
Naming Scheme,  
**September 2002**

[Adobe .pdf](#) (204 KB)

[Zipped .pdf file](#) (177 KB)

---

**SP 800-50** Building an Information Technology Security Awareness and Training Program,  
**October 2003**

[Adobe .pdf](#) (4,131 KB)  
[Zipped .pdf file](#) (3,565 KB)

---

**SP 800-49** Federal S/MIME V3 Client Profile,  
**November 2002**

[Adobe .pdf](#) (151 KB)  
[Zipped .pdf file](#) (112 KB)

---

**SP 800-48** Wireless Network Security: 802.11, Bluetooth, and Handheld Devices,  
**November 2002**

[Adobe .pdf](#) (1,027 KB)  
[Zipped .pdf file](#) (780 KB)

---

**SP 800-47** Security Guide for Interconnecting Information Technology Systems,  
**September 2002**

[Adobe .pdf](#) (729 KB)  
[Zipped .pdf file](#) (505 KB)

---

**SP 800-46** Security for Telecommuting and Broadband Communications,  
**September 2002**

[Adobe pdf](#) (3,779 KB)  
[Zipped .pdf file](#) (2,156 KB)

---

**SP 800-45** Guidelines on Electronic Mail Security,  
**September 2002**

[Adobe .pdf](#) (1,098 KB)  
[Zipped .pdf file](#) (1,019 KB)

---

**SP 800-44** Guidelines on Securing Public Web Servers,  
**September 2002**

[Adobe .pdf](#) (2,183 KB)  
[Zipped .pdf file](#) (2,073 KB)

---

**SP 800-43** Systems Administration Guidance for Windows 2000 Professional,  
**November 2002**

[Download the guidance document and security templates.](#)

---

**SP 800-42**    **Guideline on Network Security Testing,  
October 2003**

[Adobe .pdf](#) (1,554 KB)  
[Zipped .pdf file](#) (1,104 KB)

---

**SP 800-41**    **Guidelines on Firewalls and Firewall Policy,  
January 2002**

[Adobe .pdf](#) (1,180 KB)

---

**SP 800-40**    **Procedures for Handling Security Patches,  
September 2002**

[Adobe .pdf](#) (3,773 KB)  
[Zipped .pdf file](#) (1,949 KB)

---

**SP 800-38C**    **Recommendation for Block Cipher Modes of Operation: the CCM Mode for  
Authentication and Confidentiality,  
May 2004**

[Adobe .pdf](#) (104 KB)

---

**Draft SP  
800-38B**    *Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation:  
the RMAC Authentication Mode is still a DRAFT Publication - [click here to go directly  
to the DRAFTS page on CSRC.](#)*

---

**SP 800-38A**    **Recommendation for Block Cipher Modes of Operation - Methods and  
Techniques,  
December 2001**

[Adobe .pdf](#) (225 KB)

---

**SP 800-37**    **Guide for the Security Certification and Accreditation of Federal Information  
Systems,  
May 2004**

[Adobe .pdf](#) (738 KB)

---

**SP 800-36**    **Guide to Selecting Information Security Products,  
October 2003**

[Adobe .pdf](#) (464 KB)  
[Zipped .pdf file](#) (339 KB)

---

**SP 800-35** Guide to Information Technology Security Services,  
**October 2003**

[Adobe .pdf](#) (2,920 KB)  
[Zipped .pdf file](#) (2,426 KB)

---

**SP 800-34** Contingency Planning Guide for Information Technology Systems,  
**June 2002**

[Adobe .pdf](#) (1,937 KB)  
[Zipped Adobe .pdf](#) (1,164 KB)

---

**SP 800-33** Underlying Technical Models for Information Technology Security,  
**December 2001**

[Adobe .pdf](#) (453 KB)

---

**SP 800-32** Introduction to Public Key Technology and the Federal PKI Infrastructure,  
**February 2001**

[Adobe .pdf](#) (256 KB)

---

**SP 800-31** Intrusion Detection Systems (IDS),  
**November 2001**

[Adobe .pdf](#) (851 KB)

---

**Draft SP 800-30 Rev. A** *DRAFT Special Publication 800-30 Rev A, Risk Management Guide for Information Technology Systems is still a DRAFT Publication - [click here to go directly to the DRAFTS page on CSRC](#).*

---

**SP 800-30** Risk Management Guide for Information Technology Systems,  
**July 2002**

[Adobe .pdf](#) (479 KB)

---

**SP 800-29** A Comparison of the Security Requirements for Cryptographic Modules in  
FIPS 140-1 and FIPS 140-2,  
**June 2001**

[Adobe .pdf](#) (274 KB)

---

**SP 800-28** Guidelines on Active Content and Mobile Code,  
**October 2001**

[Adobe .pdf](#) (498 KB)

---

**SP 800-27 Rev. A** Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A,  
**June 2004**

[Adobe .pdf](#) (291 KB)

---

**SP 800-26** Security Self-Assessment Guide for Information Technology Systems,  
**November 2001**

[Adobe .pdf](#) (1,522 KB)  
[MS Word .doc](#) (922 KB)

---

**SP 800-25** Federal Agency Use of Public Key Technology for Digital Signatures and Authentication,  
**October 2000**

Choose 1 of 2 ways to download document  
1. [Adobe .pdf](#) (130 KB)  
2. [MS Word .doc](#) (421 KB)

---

**SP 800-24** PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does,  
**August 2000**

[Adobe .pdf](#) (225 KB)

---

**SP 800-23** Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products,  
**August 2000**

Choose 1 of 3 ways to download document  
1. [Adobe .pdf - Complete document](#) (837 KB)  
2. [Part 1 of 3 .pdf file](#) (419 KB)  
[Part 2 of 3 .pdf file](#) (160 KB)  
[Part 3 of 3 .pdf file](#) (261 KB)  
3. [Complete zipped .pdf files](#) (803 KB)

---

**SP 800-22** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,  
**October 2000**

Revised: May 15, 2001:  
[Adobe .pdf](#) (1,422 KB)  
[Errata sheet for originally published version](#) (.pdf file)

---

**SP 800-21** Guideline for Implementing Cryptography in the Federal Government,  
**November 1999**

[Adobe .pdf](#) (612 KB)

---

**SP 800-20** Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures,  
**Revised April 2000**

[Adobe .pdf](#) (1,246 KB)

---

**SP 800-19** Mobile Agent Security,  
**October 1999**

[Adobe .pdf](#) (136 KB)

---

**SP 800-18** Guide for Developing Security Plans for Information Technology Systems,  
**December 1998**

2 different file formats:  
[MS Word .doc](#) (540 KB)  
[Adobe .pdf](#) (306 KB)

Letter from CIO Council Security Committee

[Adobe .pdf](#) (31 KB)

---

**SP 800-17** Modes of Operation Validation System (MOVS): Requirements and Procedures,  
**February 1998**

[Adobe .pdf](#) (406 KB)

---

**SP 800-16** Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172),  
**April 1998**

broken down into 3 parts:  
Pt. 1 - document: [Adobe .pdf](#) (845 KB)  
Pt. 2 - Appendix A-D: [Adobe .pdf](#) (96 KB)  
Part 3 - Appendix E: [Adobe .pdf](#) (374 KB)

---

**SP 800-15** Minimum Interoperability Specification for PKI Components (MISPC),  
Version 1,  
**January 1998**

3 different file formats:  
[Adobe .pdf](#) (278 KB)  
[MS Word .doc](#) (339 KB)  
[Postscript file](#) (886 KB)

---

**SP 800-14** Generally Accepted Principles and Practices for Securing Information Technology Systems,  
**September 1996**

3 different file formats:

[Postscript file \(480 KB\)](#)  
[WordPerfect file \(182 KB\)](#)  
[Adobe .pdf \(188 KB\)](#)

**SP 800-13** Telecommunications Security Guidelines for Telecommunications Management Network,  
**October 1995**

[WordPerfect file \(217 KB\)](#)

**SP 800-12** An Introduction to Computer Security: The NIST Handbook,  
**October 1995**

[800-12 in .HTML format](#)

[Postscript File 1 of 5 \[602 KB\]](#)  
[Postscript File 2 of 5 \[3,051 KB\]](#)  
[Postscript File 3 of 5 \[1,345 KB\]](#)  
[Postscript File 4 of 5 \[575 KB\]](#)  
[Postscript File 5 of 5 \[1,247 KB\]](#)  
[Adobe .PDF File \[1,685 KB\]](#)  
[Word .doc Ch. 14-20 \[313 KB\]](#)  
[Word .doc extra of document \[18 KB\]](#)

### Archived Special Publications from 500 & 800 Series

#### Archived Special Publications:

The following Special Publications are no longer available on the CSRC website to view and/or download. If for some reason you still need to refer to a particular archived Special Publication, we can e-mail it to you. Please send e-mail to [Pat O'Reilly](#). In the e-mail please specify which Special Publication number you need. If we have the archived electronic file we can send it to you, if not we can send you a paper copy by postal mail. Please look at list below to see which document you need, and if you see that the document you need is only available in paper format, in your e-mail please include your postal address so we can mail out a paper copy to you quicker. NOTE: Due to e-mail volume, it may take a couple days to get back to you. Thanks for understanding.

These publications we have electronic copies:

#### 500 Series

- **SP 500-166** Computer Viruses and Related Threats: A Management Guide, August 1989
- **SP 500-169** Executive Guide to the Protection of Information Resources, 1989
- **SP 500-170** Management Guide to the Protection of Information Resources, 1989
- **SP 500-171** Computer Users' Guide to the Protection of Information Resources, 1989
- **SP 500-174** Guide for Selecting Automated Risk Analysis Tools, October 1989
- **SP 500-189** Security in ISDN, September 1991

#### 800 Series

- **SP 800-2** Public-Key Cryptography, April 1991
- **SP 800-3** Special Publication 800-3: Establishing a Computer Security Incident Response Capability (CSIRC), November 1991  
*As of January 2004, 800-3 has been superseded by 800-61 Computer Security Incident Handling Guide*
- **SP 800-4:** Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, March 1992  
*As of October 2003, 800-4 has been superseded by 800-64 Security Considerations in the Information System Development Life Cycle*
- **SP 800-5** A Guide to the Selection of Anti-Virus Tools and Techniques, December 1992
- **SP 800-6** Automated Tools for Testing Computer System Vulnerability, December 1992



- **SP 800-7** Security in Open Systems, July 1994
- **SP 800-8** Security Issues in the Database Language SQL, August 1993
- **SP 800-9** Good Security Practices for Electronic Commerce, Including Electronic Data Interchange, December 1993
- **SP 800-10** Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, December 1994
- **SP 800-11** The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security, February 1995

The documents listed **below** (500 series), we only have "paper" copies of. (No electronic file is available for the documents listed below.) If you want us to send you a paper copy of any of these documents listed below, please include your postal address in the e-mail. That way we can ship out the document to you quicker. Thanks. NIST Computer Security Webmaster.

- **SP 500-61** Maintenance Testing for the Data Encryption Standard, August 1980
  - **SP 500-120** Security of Personal Computer Systems - A Management Guide, January 1985
  - **SP 500-133** Technology Assessment: Methods for Measuring the Level of Computer Security, October 1985
  - **SP 500-134** Guide on Selecting ADP Backup Process Alternatives, November 1985
  - **SP 500-153** Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, April 1988
  - **SP 500-156** Message Authentication Code (MAC) Validation System: Requirements and Procedures, May 1988
  - **SP 500-158** Accuracy, Integrity, and Security in Computerized Vote-Tallying, August 1988
  - **SP 500-157** Smart Card Technology: New Methods for Computer Access Control, September 1988
  - **SP 500-172** Computer Security Training Guidelines, November 1989
- Superseded by Special Publication 800-16 Information Technology Security Training Requirements: A Role- and Performance- Based Model, April 1998*

---

*Last updated: August 19, 2004*

*Page created: February 23, 2001*

[Disclaimer Notice & Privacy Statement / Security Notice](#)

Send comments or suggestions to [webmaster-csrc@nist.gov](mailto:webmaster-csrc@nist.gov)

NIST is an Agency of the U.S. Commerce Department's Technology Administration